УДК 343.7

ФИШИНГ-АТАКА КАК МЕТОД НЕСАНКЦИОНИРОВАННОГО ДОСТУПА К КОНФИДЕНЦИАЛЬНЫМ ДАННЫМ

Д. И. Шнейдерова
преподаватель кафедры уголовного процесса и криминалистики,
Могилевский институт МВД Республики Беларусь
e-mail: galuzodi@mail.ru

Д. С. Захаров
курсант 2-го курса факультета милиции,
Могилевский институт МВД Республики Беларусь
e-mail: dima_zakharov_123@mail.ru

Аннотация. *Статья посвящена анализу механизмов реализации различных видов фишинг-атак, являющихся методом несанкционированного доступа к конфиденциальным данным пользователя. Авторами дается определение фишинг-атак, приводятся их классификация и меры предупреждения.*

Ключевые слова: *фишинг, Интернет, несанкционированный доступ, конфиденциальные данные, электронная почта, вредоносное программное обеспечение.*

Annotation. *The article is devoted to the analysis of mechanisms for implementing various types of phishing attacks, which are a method of unauthorized access to confidential user data. The authors provide a definition of phishing attacks, their classification and prevention measures.*

Keywords: *phishing, Internet, unauthorized access, confidential data, email, malicious software.*

Внедрение интернет-пространства и продуктов научно-технического прогресса в повседневную жизнь современного общества приводит к развитию усовершенствованных видов киберпреступности, направленных в большей степени на завладение личными данными пользователей глобальной сети и их собственностью. Согласно данным информационного центра Министерства внутренних дел Республики Беларусь самым распространенным видом преступлений, совершаемых в сфере высоких технологий, является хищение путем использования компьютерной техники, сопряженное с несанкционированным доступом к компьютерной информации, а именно к конфиденциальным данным пользователей сети Интернет. Так, за 2019 год по Республике Беларусь было зарегистрировано 3 573 преступления, по которым возбуждены уголовные дела по частям 2–4 ст. 212 Уголовного кодекса Республики Беларусь с указанным квалифицирующим признаком. По сравнению с 2018 годом, количество рассматриваемых преступлений увеличилось к 2020 году на 3 393 факта (т. е. в 19,9 раз; прирост составил 1 885 %).

Одним из методов несанкционированного доступа к конфиденциальной информации пользователей является фишинг-атака, которая представляет собой способ противоправного получения личных данных пользователей (логинов, паролей, приватных ключей и других) путем внедрения вредоносного программного обеспечения на используемые устройства (компьютеры, мобильные телефоны) или побуждения посредством обмана к вводу данных для авторизации на фальшивых сайтах-близнецах в сети Интернет. Конфиденциальные данные позволяют преступникам осуществить беспрепятственный доступ к электронным и криптовалютным кошелькам, банковским картам, мобильным и интернет-банкингам с целью хищения денежных средств пользователя, в том числе виртуальных (криптовалюты, токенов).

Следует отметить, что фишеры в рамках своей преступной деятельности используют различные методы психологического воздействия, делая упор на такие черты личности, как доверчивость, жадность, лень, чувство сострадания, поспешность в принятии важных решений, желание получить «легкий» заработок или приумножить свое благосостояние. При этом в большинстве случаев киберпреступники прикрываются именами и логотипами крупных знаменитых компаний, почтовых сервисов, массовых социальных сетей, работников органов исполнительной власти, банков, партнеров по бизнесу и других.

Фишинговые атаки могут осуществляться посредством интернет- или SMS-рассылок писем из различных виртуальных источников, информационная составляющая которых побуждает пользователя следовать указаниям и совершать необходимые преступнику действия. Приведем классификацию фишинг-атак и рассмотрим механизмы их реализации.

Возможность доступа к конфиденциальным данным пользователя может быть получена посредством создания «сайтов-близнецов», внешне схожих с оригинальными как по интерфейсу, так и по URL-адресу (т. е. адресу сайта в сети Интернет). Например, пользователю приходит уведомление на почтовый ящик о необходимости пройти повторную авторизацию, для чего следует перейти по ссылке и ввести свои учетные данные. Открыв в браузере указанную ссылку, пользователь попадает на страницу хорошо знакомого сайта с окном для авторизации, ничего не подозревая, вводит свои данные, после чего страница либо автоматически перезагружается, и появляется все то же окно авторизации, либо перенаправляет пользователя далее в учетную запись для ввода иной личной информации. При этом стоит обратить внимание, что для регистрации адреса поддельного сайта достаточно скопировать оригинальное название, заменив в нем всего лишь одну букву или символ.

По статистике, 27 % попыток всех фишинговых атак происходит через электронную почту. При этом пострадавшими оказываются не только обману-

тые пользователи, но и корпорации, владеющие знаменитыми брендовыми интернет-ресурсами. В 2019 году наблюдалось ранжирование фишинговых страниц в зависимости от устройств, использующих выход в глобальную сеть. Например, через мобильные устройства в основном распространялись фишинговые страницы социальных сетей и банков. Через электронную почту, как правило, распространялись фишинговые письма, приуроченные к периоду распродаж, например таких, как черная пятница в ноябре 2019 года. Согласно отчету израильской компании Check Point (компания занимается разработкой программ в сфере обеспечения кибербезопасности) в 2019 году больше всего пострадали такие интернет-ресурсы как Facebook (18 % фишинговых атак в мире), Yahoo (10 %), Netflix (5 %), PayPal (5 %), Microsoft (3 %), Apple (2 %), Google (2 %) и др. [1].

Еще одним способом фишинговой атаки является переход по активной ссылке, которая не перенаправляет на поддельную страницу сайта, а инициирует процесс автоматической загрузки на компьютер или мобильное устройство вредоносного программного обеспечения, способного считывать личные данные пользователя, сохраненные как в текстовых файлах, памяти браузера или интернет-банкинга, так и непосредственно вводимые через клавиатуру после загрузки вируса. Такие программы могут нарушать общий режим работы устройства, блокировать доступ к другим программам или файлам, однако в некоторых случаях они остаются фоновыми и незаметными для пользователя.

Следует отметить, что вредоносное программное обеспечение может передаваться также посредством вложенных в электронное письмо текстовых или pdf-файлов. Так пользователь получает сообщение от администрации сайта или знакомого человека с текстом, обращающим внимание на необходимость ознакомления с вложенными файлами для получения детальной информации, открытие которых активизирует загрузку вируса.

Таким образом, можно говорить о том, что в основе механизма фишинга лежит два основных способа получения конфиденциальных данных, дающих возможность злоумышленнику похитить денежные средства: либо собственноручный ввод данных на поддельных сайтах, либо загрузка вирусного программного обеспечения путем перехода по ссылке или скачивания документов различных форматов.

Несмотря на то что механизмов работы фишинга не так уж и много, хакеры совершенствуют свою деятельность в данном направлении и внедряют новые способы обмана. В связи с чем фишинг может быть классифицирован также и по адресатам, которым предназначены письма-ловушки.

Самую большую группу в данной классификации составляет спам-рассылка, рассчитанная на неограниченный круг случайно определенных поль-

зователей. Спам-сообщения могут приходить как на почтовый ящик, так и в аккаунтах социальных сетей и иметь различное смысловое содержание. Например, сообщение о рекламе розыгрыша дорогостоящих призов, о бонусах и акциях брендовых магазинов, о предоставлении купона с большой скидкой на товар, о попытках взлома аккаунта с чужого устройства, о дополнительной проверке безопасности, о получении денежного выигрыша или пополнении счета и др. Для привлечения дополнительного внимания преступники часто используют фотографии знаменитых людей и рекламируют поддельные сайты от их имени или бренда.

Противоположным спаму является целенаправленный фишинг, рассчитанный на обман определенного человека или группы людей, объединенных общими интересами. При данном виде фишинг-атак текст сообщения в большинстве случаев содержит обращение к пользователю по его имени и фамилии, имеет четко сформулированную просьбу или требование, не вызывающие сомнений. Например, требование о проверке достоверности личных данных, о блокировке взломанного электронного кошелька, о подтверждении перевода денег на банковскую карту, об оплате задолженности по какому-либо обязательству с указанием реквизитов, просьба от имени хорошо знакомого человека о денежной помощи с предоставлением данных платежной карты, о поддержке в конкурсе путем проставления «лайка» или «голоса», просмотре фотографий, требующие перехода по ссылке, и другие.

Популярным является пример письма от иностранного адвоката, сообщающего пользователю печальное известие о смерти дальнего родственника, оставившего для него большое наследство, для получения которого требуется либо переход по ссылке, либо дальнейшая переписка и отправка конфиденциальных данных.

Разновидностью целенаправленного фишинга является уэйлинг (Whaling), который направлен на обман знаменитых публичных людей, руководителей крупных организаций, банков, государственных органов с целью хищения личных данных, информации о сотрудниках и денежных средств. Примерами могут служить ссылки на жалобы клиентов, судебные повестки или другая информация. Уэйлинговые письма чаще всего используют вложенные документы, так как их наличие не вызывает сомнения у пользователя о реальности намерений бизнес-партнера или подчиненного работника.

Необходимо отметить, что на сегодняшний день хакеры применяют фишинговые схемы не только в рамках интернет-пространства, но и посредством мобильных сетей. Такой вид фишинг-обмана получил название Смишинг (SMiShing). Он концептуально очень схож с обычным фишингом, но реализует-

ся путем рассылки текстовых SMS-сообщений, содержащих ссылки на подставные сайты или зараженные вирусом мобильные приложения.

Таким образом, анализ механизмов и способов реализации фишинговых атак позволяет определить основные меры по предупреждению хищений путем использования компьютерной техники, сопряженных с несанкционированным доступом к конфиденциальным данным:

1. При получении подозрительного письма от администрации хорошо знакомого сайта, даже если по внешним признакам он идентичен настоящему, целесообразно убедиться в правильном написании как доменного имени сайта (URL-адреса), так и самого отправителя, так как чаще всего они отличаются лишь на одну-две буквы (символа). Только после этого можно вводить свои личные данные, открывающие доступ к денежным ресурсам.

2. Следует внимательно ознакомиться и с содержанием письма. В большинстве случаев злоумышленники требуют активных действий от пользователя под угрозой ограничения его прав по использованию конкретного ресурса, что никогда не будут делать сотрудники реальной администрации. В данном случае целесообразно связаться с представителями сайта или организации и уточнить полученную информацию.

3. Внимания требуют и стилистические признаки изложения текста. Некоторые преступники составляют сообщения на иностранных языках, знакомых не всем пользователям. Такие письма сопровождаются неграмотным техническим переводом, при котором перед пользователем появляется несвязный текст с низкой смысловой нагрузкой. Кроме того, настораживающим является и отсутствие факта посещения когда-либо пользователем сайтов на незнакомом языке.

4. Необходимо обеспечить и техническую защиту устройства, с которого пользователь осуществляет выход в Интернет посредством установления антивирусных программ с функцией выявления и блокировки фишинговых атак, а также осуществлять периодическую проверку файлов, хранящихся на устройстве, на наличие скрытых угроз и фоновых процессов.

5. Если дело касается взаимоотношений между знакомыми людьми, то лучше лишний раз убедиться в необходимости оказания человеку помощи посредством телефонной связи или личной встречи.

Резюмируя вышеизложенное, необходимо отметить, что на сегодняшний день безопасность конфиденциальных данных, предоставляющих доступ к денежным и виртуальным средствам, зависит в большей степени от самих пользователей. Однако представляется целесообразным правоохранительным органам проводить информационно-аналитическую работу с гражданами посредством участия с докладами в рамках дней информирования трудовых коллекти-

вов и учащихся образовательных учреждений, а также размещать информацию предупреждающего характера на информационных стендах и сайте ведомства.

1. Названы самые «опасные» бренды, которыми прикрываются интернет-мошенники [Электронный ресурс] // Новостной интернет-портал «News-Life». URL: https://news-life.pro/234105171/ (дата обращения: 28.02.2020). Вернуться к статье